

UNITED STATES DISTRICT COURT

for the

District of

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. MR 23-1491



APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

located in the District of , there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

The application is based on these facts:

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
(specify reliable electronic means).

Date:

Judge's signature

City and state:

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Shayne Beckford, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (“SA”) with the Department of Homeland Security (“DHS”), Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”) and have been employed as such since March 2019. I am currently assigned to the Albuquerque, New Mexico Deputy Special Agent in Charge (“DSAC”) field office.

3. I am a graduate of the Federal Law Enforcement Training Center (FLETC) and a graduate of Homeland Security Investigations Special Agent Training (HSISAT) in Glynco, Georgia. I received a Bachelor of Arts in Law & Justice in 2009 and a Master of Arts in Criminal Justice in 2012 from Rowan University. Prior to becoming a Special Agent, I worked for New Mexico State Police (NMSP) as a law enforcement officer for approximately 7 years.

4. While employed with NMSP, I was a narcotics agent for approximately two years and participated in numerous drug and criminal investigations. I have received extensive training and practical experience pertaining to federal criminal procedures, federal criminal statutes, United States Immigration and Nationality law, United States Customs laws and regulations, and other federal and state laws pertaining to, but not limited to: Alien Smuggling/Human

Trafficking, fraudulent document manufacture and sales; the importation and distribution of controlled substances, firearms, commercial fraud, and conspiracy.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched consists of one cellular telephone, as described in Attachment A and B (hereafter referred to as the “Device”) and is identified as follows:

- A black iPhone identified by IMEI: 354065526887943. This Device is currently located in evidence at the HSI Albuquerque Office.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

DRUG TRAFFICKING AND CELLULAR DEVICES

8. Based upon my training and experience, and on my consultation with other law enforcement officers experienced in investigations regarding conspiracy to manufacture, distribute and possess with intent to distribute controlled substances, I have learned the following:

- a. Those who possess illegal drugs for distribution often use electronic devices such as wireless or cellular telephones and smartphones. Such electronic devices are often used to communicate with coconspirators and customers through the telephone’s standard capabilities to call and text, as well as through smartphone applications (“apps”) such as WhatsApp, Snapchat, Pinger, Marco Polo and Facebook, which allow users to send and receive digital communications in various forms such as voice calls, text messages, image and video sharing, and live video conversations.

Records of these communications, text messages, and contact lists are frequently retained and stored on those electronic devices and within those apps. Based upon my training, experience, and knowledge of this investigation, I believe that such evidence and information is likely to be found in the Device.

b. Individuals involved in the illegal trafficking of controlled substances often maintain documents, records, and other evidence of their transactions in a manner similar to the record keeping procedures of legitimate businesses. Even after the drugs are sold, documentary records are often maintained for long periods of time, even years, to memorialize past transactions, the status of accounts receivable and accounts payable, and the names and telephone numbers of suppliers, customers and co-conspirators. These records may be maintained on paper, in the form of business and personal ledgers and diaries, calendars, memoranda, pay/owe sheets, IOUs, miscellaneous notes, money orders, customer lists and telephone address books. These records can reflect names, addresses and/or telephone numbers of associates and co-conspirators, the sale and purchase of controlled substances including precursors, customer lists and amounts of money owed to the trafficker by customers and by the trafficker to his/her suppliers. All such records can also be produced and/or stored on cellular telephones and evidence of these transactions is often contained within cellular phones.

c. Drug dealers often travel domestically and internationally to facilitate their trafficking. Evidence of foreign and domestic travel by persons engaged in illegal drug trafficking includes travel itineraries, airline tickets, hotel and gas receipts, and passports and visas and their contents. Many of these items are accessible via the internet and can be downloaded and saved on the computer or other media such as cellular phones.

d. Drug trafficking is a crime that necessarily involves at least two people – a buyer and a seller. Prior to engaging in the drug transaction, the buyer and seller must communicate and discuss the type of drug to be sold, the quantity, the price, and the location where the sale will take place. I know that drug dealers and their customers make use of cellular phones and smartphones to conduct these necessary communications.

e. Information stored in electronic form on cellular telephones can provide evidence of drug trafficking and the identity of associates. For example, numbers stored on cellular telephones (such as Caller ID lists reflecting recently received calls, speed dial lists of names and/or telephone numbers, and logs of outgoing and incoming calls) can provide evidence of who the drug dealer is calling, and thus the identity of associates.

f. Drug dealers often take, or cause to be taken, photographs and/or videos of themselves, their associates, their property, drug trafficking records, records of financial transactions involving drug trafficking proceeds, their drugs, and firearms. They usually take these photographs and/or videos with their cellular phones and store them in those cellular phones.

g. I know that those engaged in drug trafficking have access to, and utilize, numerous cellular telephones, often at the same time in an effort to avoid law enforcement monitoring.

h. Electronic information can remain on computer storage media, such as within cellular phones, for an indefinite period of time. I am aware that even when a user attempts to delete records from computer storage media, the records may still exist and be recovered through computer forensic techniques.

PROBABLE CAUSE

9. On August 1, 2023, at approximately 1809 hours, Bureau of Indian Affairs (BIA) officer Nicholas Jackson was on duty, in full uniform, in his marked K-9 patrol unit. Officer Jackson was conducting speed enforcement on the eastbound lanes of Interstate 40 near mile marker 120 utilizing his department-issued Kustom Signal Pro-Lite+ (LIDAR) speed-measuring device. Officer Jackson observed what was later identified as a gray Wagoneer 4-door (SUV) bearing Indiana License Plate “FL253ACZ”, traveling in the left lane at 83 miles per hour, in excess of the posted speed limit of 75 mph.

10. Prior to engaging his emergency equipment to initiate a traffic stop Officer Jackson conducted a record’s check on the registration which returned “No Record / Not on File.” Officer Jackson then activated his emergency lights and Dash Camera and conducted a traffic stop. Upon reaching the front passenger window, Officer Jackson immediately detected an odor of burnt and unburnt marijuana emanating from vehicle.

11. Officer Jackson identified himself and requested the driver, who was later identified as HYLER-Williams, to walk to his unit. While at the police unit, in conversation with officer Jackson, HYLER-Williams stated the following:

- a. he and BERRY were driving from Phoenix, Arizona.
- b. he knew his license was suspended and was “just helping to drive.”
- c. he smoked marijuana earlier in the day.
- d. he did not have any luggage besides a grocery bag of dirty clothes.

12. Officer Jackson conducted a probable cause search based on the immediate odor of burnt and unburnt marijuana emanating from vehicle while at the passenger window. A search of the vehicle resulted in Officer Jackson locating a brown box on the 3rd row with a vacuum-

sealed bag containing a large brick shaped bundle and two oddly shaped items in birthday wrapping paper. Officer Jackson knew the large brick-shaped bundle is consistent with the appearance of pressed bricks of narcotics based on his training and experience in narcotics. Officer Jackson also located a Welch's fruit snacks box with contained heat-sealed bags concealing an unknown substance further concealed inside baby diapers.

13. In the center console of the vehicle, Officer Jackson located a green leafy substance secured in a clear plastic baggie next to an unknown amount of United States currency. Both HYLER-Williams and BERRY were taken into custody and transported to the Albuquerque HSI office. The vehicle also was taken to the Albuquerque HSI office, and, once there, evidence was removed from the vehicle and was processed.

14. SA Beckford was contacted to assisted Officer Jackson with the investigation. At the Albuquerque HSI office, SA Beckford noticed four cellular devices, including the Device, next to the suspected narcotics and an unknown amount of US currency some of which. In a photo taken by Officer Jackson, all four of the cellular devices were located on top on the center console. A handheld narcotics analyzer was utilized to test one of four packages that were identically wrapped with baby diapers and heat sealed in a clear plastic. When the package was opened, SA Beckford observed a clear crystal-like substance. This substance tested presumptively positive for methamphetamine and weighed 962 grams.

15. The other three packages that were opened displayed blue in color pills with the marker "M/30," and weighed a total of 2.8 kilograms. Each package of pills was tested and presumptively tested positive for fentanyl. The vacuum-sealed bag containing the large brick shaped bundle was cut open, and the exterior wrapping of the brick was tested utilizing the handheld narcotics analyzer. This substance tested positive for fentanyl and weighed 1.04

kilograms. The green leafy substance identified by my training and experience as marijuana weighed approximately 1.8 grams.

16. Based on the events described above, there is probable cause to believe that the Device will contain evidence of BERRY's drug trafficking activities, specifically violations of 21 U.S.C. §§ 841 and 846.

17. The Device is currently in the lawful possession of HSI. They came into the HSI's possession in the following way: the Device was brought to the HSI Albuquerque office by Officer Jackson upon the arrest the target on Tuesday August 1, 2023. The black iPhone was located on the center console arm rest of target vehicle closest to the front passenger seat.

18. The Device is currently in storage at the HSI Albuquerque Office. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of HSI.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless

telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital

data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This

removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

20. Based on my training, experience, and research, I know that the Device has capabilities that allows it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachments A to seek the items described in Attachment B.

26. The affidavit has been reviewed by AUSA Katherine Lewis.

Respectfully submitted,



Shayne Beckford
Special Agent
Homeland Security Investigation

Subscribed and sworn telephonically and signed electronically on August 4, 2023



B. PAUL BRIONES
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is black iPhone identified by IMEI:
354065526887943. This Device is currently located in evidence at HSI Albuquerque
Office.

This warrant authorizes the forensic examination of this device for the purpose of
identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and information on the Device described in Attachment A that relate to violations of 21 U.S.C. §§ 841 and 846 including:
 - a. data and information identifying co-conspirators, customers, and suppliers;
 - b. communications between co-conspirators, customers, and suppliers;
 - c. data and information regarding the types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - d. data and information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - e. photographs and/or videos;
 - f. financial records or other information regarding the expenditure or disposition of proceeds from the distribution of controlled substances including all bank records, checks, credit card bills, account information, and other financial records; and
 - g. records of travel.
2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and

instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.